
CESG

Biometric Authentication

Where does it Fit in the UK e-Government Authentication Framework?

Philip Statham - CESG Biometrics Programme Manager

Brian Holman – ID&A Policy Developer

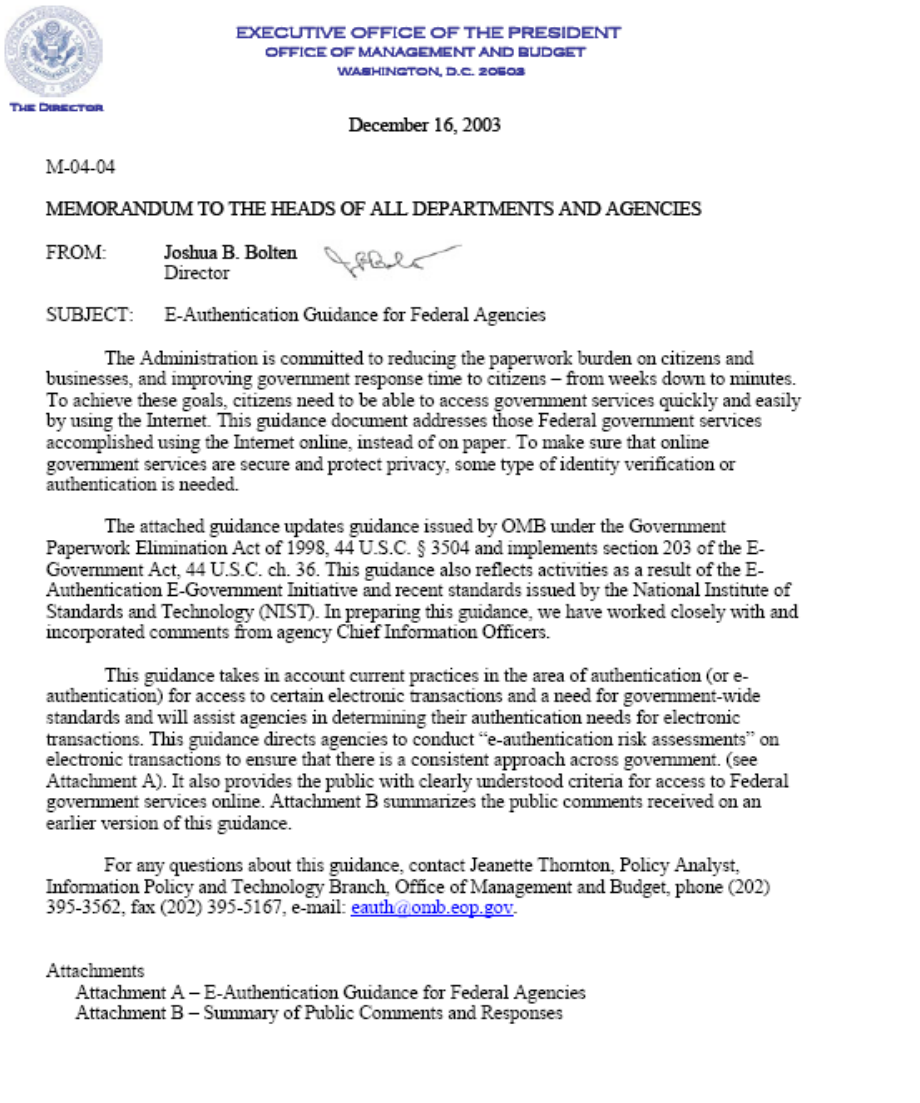
philip.statham@cesg.gsi.gov.uk

brian.holman@cesg.gsi.gov.uk

Outline

- Compare US and UK e-Authentication Guidance
- Features of Password, Token, Biometric authentication mechanisms
- Comparing and quantifying authentication mechanisms
- Approaches to authentication policy
- Future CESG authentication policy advice for UK Government

M-04-04 E-Authentication Guidance for Federal Agencies



EXECUTIVE OFFICE OF THE PRESIDENT
OFFICE OF MANAGEMENT AND BUDGET
WASHINGTON, D.C. 20503

THE DIRECTOR

December 16, 2003

M-04-04

MEMORANDUM TO THE HEADS OF ALL DEPARTMENTS AND AGENCIES

FROM: Joshua B. Bolten
Director

SUBJECT: E-Authentication Guidance for Federal Agencies

The Administration is committed to reducing the paperwork burden on citizens and businesses, and improving government response time to citizens – from weeks down to minutes. To achieve these goals, citizens need to be able to access government services quickly and easily by using the Internet. This guidance document addresses those Federal government services accomplished using the Internet online, instead of on paper. To make sure that online government services are secure and protect privacy, some type of identity verification or authentication is needed.

The attached guidance updates guidance issued by OMB under the Government Paperwork Elimination Act of 1998, 44 U.S.C. § 3504 and implements section 203 of the E-Government Act, 44 U.S.C. ch. 36. This guidance also reflects activities as a result of the E-Authentication E-Government Initiative and recent standards issued by the National Institute of Standards and Technology (NIST). In preparing this guidance, we have worked closely with and incorporated comments from agency Chief Information Officers.

This guidance takes in account current practices in the area of authentication (or e-authentication) for access to certain electronic transactions and a need for government-wide standards and will assist agencies in determining their authentication needs for electronic transactions. This guidance directs agencies to conduct "e-authentication risk assessments" on electronic transactions to ensure that there is a consistent approach across government. (see Attachment A). It also provides the public with clearly understood criteria for access to Federal government services online. Attachment B summarizes the public comments received on an earlier version of this guidance.

For any questions about this guidance, contact Jeanette Thornton, Policy Analyst, Information Policy and Technology Branch, Office of Management and Budget, phone (202) 395-3562, fax (202) 395-5167, e-mail: eauth@omb.eop.gov.

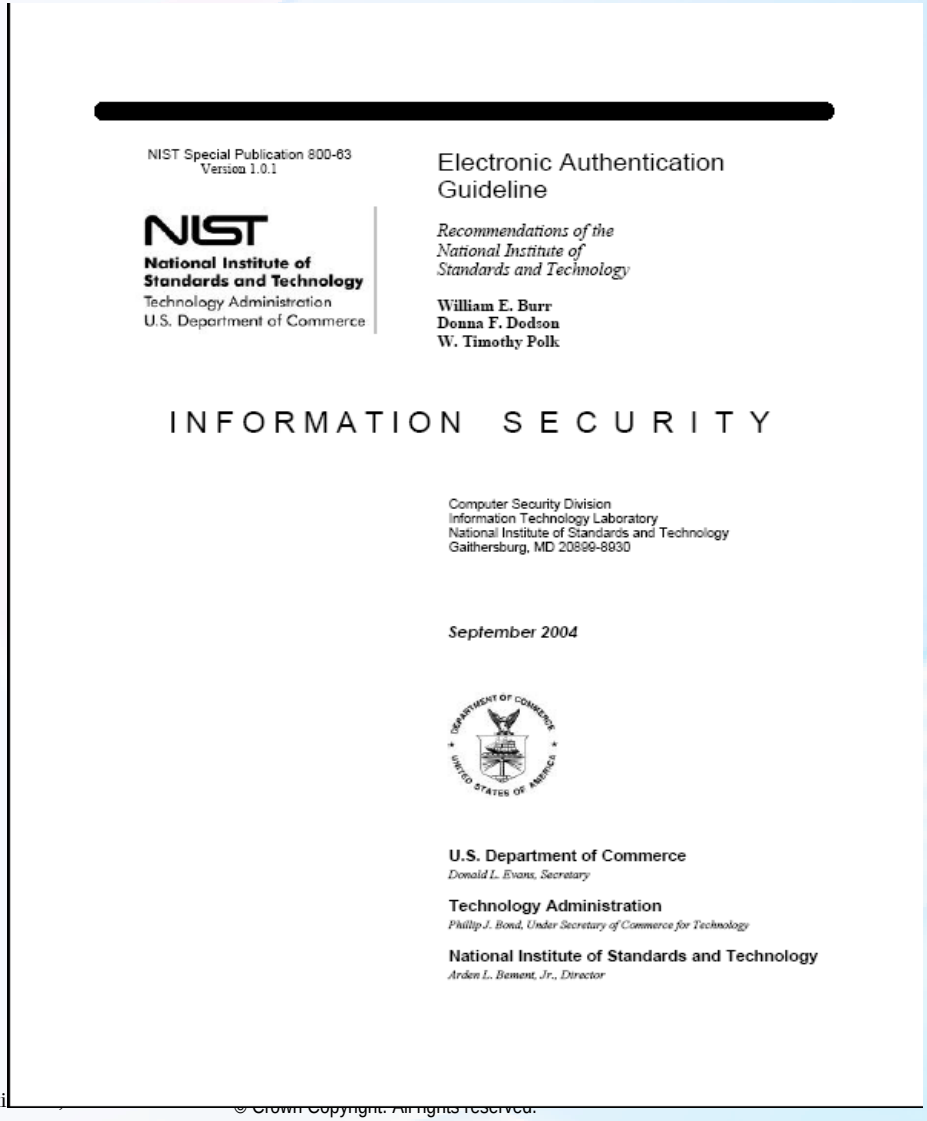
Attachments
Attachment A – E-Authentication Guidance for Federal Agencies
Attachment B – Summary of Public Comments and Responses

M-04-04 E-Authentication Guidance for Federal Agencies

4 authentication assurance levels

- Level 1: Little or no confidence in the asserted identity's validity.
- Level 2: Some confidence in the asserted identity's validity.
- Level 3: High confidence in the asserted identity's validity.
- Level 4: Very high confidence in the asserted identity's validity.

NIST SP 800-63 Electronic Authentication Guideline



NIST Special Publication 800-63
Version 1.0.1

NIST
National Institute of Standards and Technology
Technology Administration
U.S. Department of Commerce

Electronic Authentication Guideline

Recommendations of the National Institute of Standards and Technology

William E. Burr
Donna F. Dodson
W. Timothy Polk

INFORMATION SECURITY

Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology
Gaithersburg, MD 20899-8930

September 2004

U.S. Department of Commerce
Donald L. Evans, Secretary

Technology Administration
Phillip J. Bond, Under Secretary of Commerce for Technology

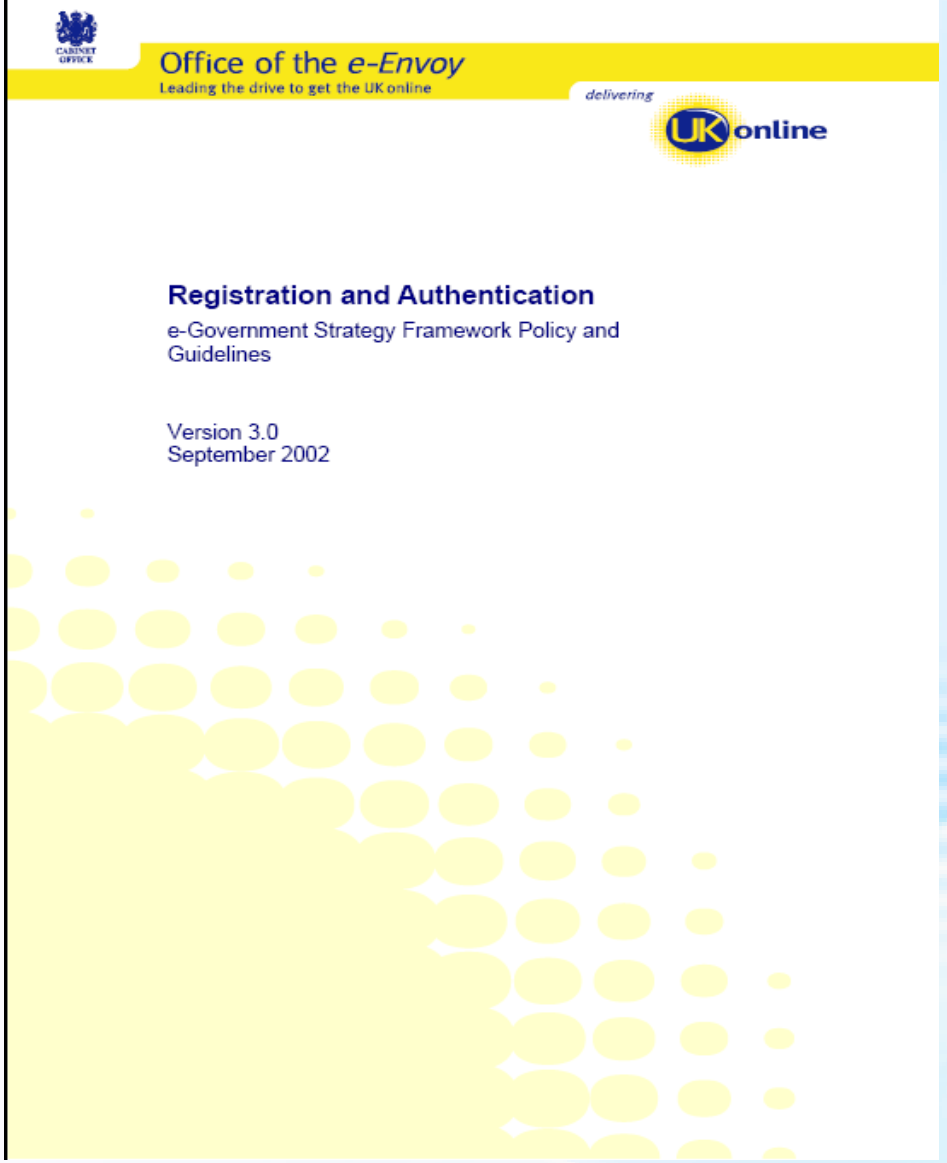
National Institute of Standards and Technology
Arden L. Bement, Jr., Director

NIST SP 800-63 Electronic Authentication Guideline

Table 2. Token Types Allowed at Each Assurance Level

Token type	Level 1	Level 2	Level 3	Level 4
Hard crypto token	√	√	√	√
One-time password device	√	√	√	
Soft crypto token	√	√	√	
Passwords & PINs	√	√		

UK e-Government Registration and Authentication Strategy



e-Government Strategy Framework Policy and Guidelines

Registration Level - Degree of confidence in an asserted real-world identity

Authentication Level - Degree of confidence in an electronic identity presented to a service provider by means of a credential

- **Defined in terms of damage caused by breaches**
  - **Level 0 – minimal damage**
  - **Level 1 – minor damage**
  - **Level 2 – significant damage**
  - **Level 3 – substantial damage**

e-Government Strategy Framework Policy and Guidelines – Registration Requirements

Level	Personal Statement	Documentary Evidence (e.g. Passport or ID Card)	3rd Party Corroboration	Evidence of activity in community
0	-	-	-	-
1	✓	✓	or ✓	-
2	✓	✓	-	✓
3	✓	✓	✓	✓✓

e-Government Strategy Framework Policy and Guidelines – Authentication Requirements

Level	Password	Biometric	Smart Token	Digital Certificate	Private Key
0	-	-	-	-	-
1	✓	or ✓	-	-	-
2	✓	or ✓	-	✓	✓
3	✓	or ✓	✓	✓	✓

Comparison of US and UK Risk Criteria

- US M04-04
  - Potential impact of ***inconvenience, distress, or damage to standing or reputation***
  - Potential impact of ***financial loss***
  - Potential impact of ***harm to agency programs or public interests***
  - Potential impact of ***unauthorized release of sensitive information***
  - Potential impact to ***personal safety***
  - The potential impact of ***civil or criminal violations***

- UK e-Gov *Authentication Policy*
  - Potential inconvenience to any party
  - Potential distress being caused to any party
  - Potential damage to any party's standing or reputation
  - Potential financial loss to any party
  - Potential impact of the release of personally or commercially sensitive data to third parties
  - Potential risk to any party's personal safety
  - Potential for assistance in the commission of or hindrance to the detection of serious crime

Comparison of US And UK Authentication Levels

- US M04-04 – Defined in terms of confidence of asserted identity

- Level 1: Little or no confidence in the asserted identity's validity
- Level 2: Some confidence in the asserted identity's validity
- Level 3: High confidence in the asserted identity's validity
- Level 4: Very high confidence in the asserted identity's validity

- UK e-Gov *Authentication Policy* - Defined in terms of damage caused by breaches

- Level 0 – minimal damage
- Level 1 – minor damage
- Level 2 – significant damage
- Level 3 – substantial damage

Conclusion

- UK and US specifications of authentication levels are orthogonal
  - UK defines levels in terms of damage
  - US defines levels in terms of confidence of identity
- However the end results are much the same
  - UK Levels 0-3 correspond to US Levels 1-4
- UK and US specifications of authentication requirements are orthogonal
  - UK specifies what is required
  - US specifies what is allowed

Password / Biometric Entropy and Strength of Function

Password Entropy – SP 800-63

Table A.1 – Estimated Password Guessing Entropy in bits vs. Password Length

	User Chosen			Randomly Chosen		
	94 Character Alphabet			10 char. alphabet		94 char alphabet
Length Char.	No Checks	Dictionary Rule	Dict. & Comp. Rule			
1	4	-	-	3	3.3	6.6
2	6	-	-	5	6.7	13.2
3	8	-	-	7	10.0	19.8
4	10	14	16	9	13.3	26.3
5	12	17	20	10	16.7	32.9
6	14	20	23	11	20.0	39.5
7	16	22	27	12	23.3	46.1
8	18	24	30	13	26.6	52.7
10	21	26	32	15	33.3	65.9
12	24	28	34	17	40.0	79.0
14	27	30	36	19	46.6	92.2
16	30	32	38	21	53.3	105.4
18	33	34	40	23	59.9	118.5
20	36	36	42	25	66.6	131.7
22	38	38	44	27	73.3	144.7
24	40	40	46	29	79.9	158.0
30	46	46	52	35	99.9	197.2
40	56	56	62	45	133.2	263.4

Password SOF

- SOF relates to probabilistic mechanisms
- For passwords this maps to the probability of guessing the password
  - Password SOF defined by entropy
    - e.g. 4 digit PIN has raw entropy of 10000
    - Real entropy may be less (restricted subsets, non random choice etc.)
    - Also effective entropy reduced by multiple attempts
- Note: CC CEM Annex B.8.3 example rates a 4 Digit PIN as SOF Basic

Biometric Entropy and Password Equivalence

- Biometric authentication has a probability of chance (false) match, given by the FAR
- So we infer that biometric entropy is related to FAR (for authentication)
- How do we compare biometric entropy to password entropy?
  - Direct equality e.g. FAR = PW raw entropy?
  - Makes no allowance for different potential for retries in the 2 cases
- Need to equate real rather than raw entropies

Password/Biometric Comparison

Illustrative Example

- Password – 4 Digit PIN
  - Raw entropy 10000
  - Real entropy ~5000 (see CC CEM Annex B.8.3)
  - Assume 100 retries (over period of time)
  - Chance of success 1 in 50
  - **N.B. CC CEM B.8.3 rates this as SOF Basic**
- Biometric – FAR 1%
  - Raw entropy 100
  - Real entropy = 100 / no of attempts possible
  - Same order of magnitude as 4 digit PIN example

Common Methodology for Information Technology Security Evaluation
Biometric Evaluation Methodology Supplement [BEM]

Table 11: SOF defined in Terms of FAR

Strength of Function Level	Maximum FAR
SOF-Basic	0.01 (1 in 100)
SOF-Medium	0.0001 (1 in 10,000)
SOF-High	0.000001 (1 in 1,000,000)

Authentication Security

Authentication Threats

- Casual (Zero Effort) attacks
  - Discrimination, entropy – ability to distinguish between individuals
- Human/Procedural failures
  - Social engineering
  - “Easy” secrets
  - Failure to guard secrets
  - Corrupt users/administrators
- Technical attacks
  - Direct attacks against authentication mechanism
  - Indirect attacks against supporting infrastructure
    - Transmission paths
    - Databases

Security is Multi-Dimensional

- Discrimination/Entropy Strength
- Binding Strength
- Human/Procedural Security
- Resistance to Technical Attack

Passwords

- Technically strong
  - Long string = High entropy
  - Cryptographically strong algorithms – can't be reverse engineered
- Procedurally weak
  - Short passwords = Low entropy
  - Easy-to-guess passwords = Low/zero entropy
  - Written down = Zero entropy
  - Divulged to colleagues = Zero entropy
  - Vulnerable to social engineering attacks = Zero entropy
- Password security paradox
  - Increased technical strength → decreased procedural strength

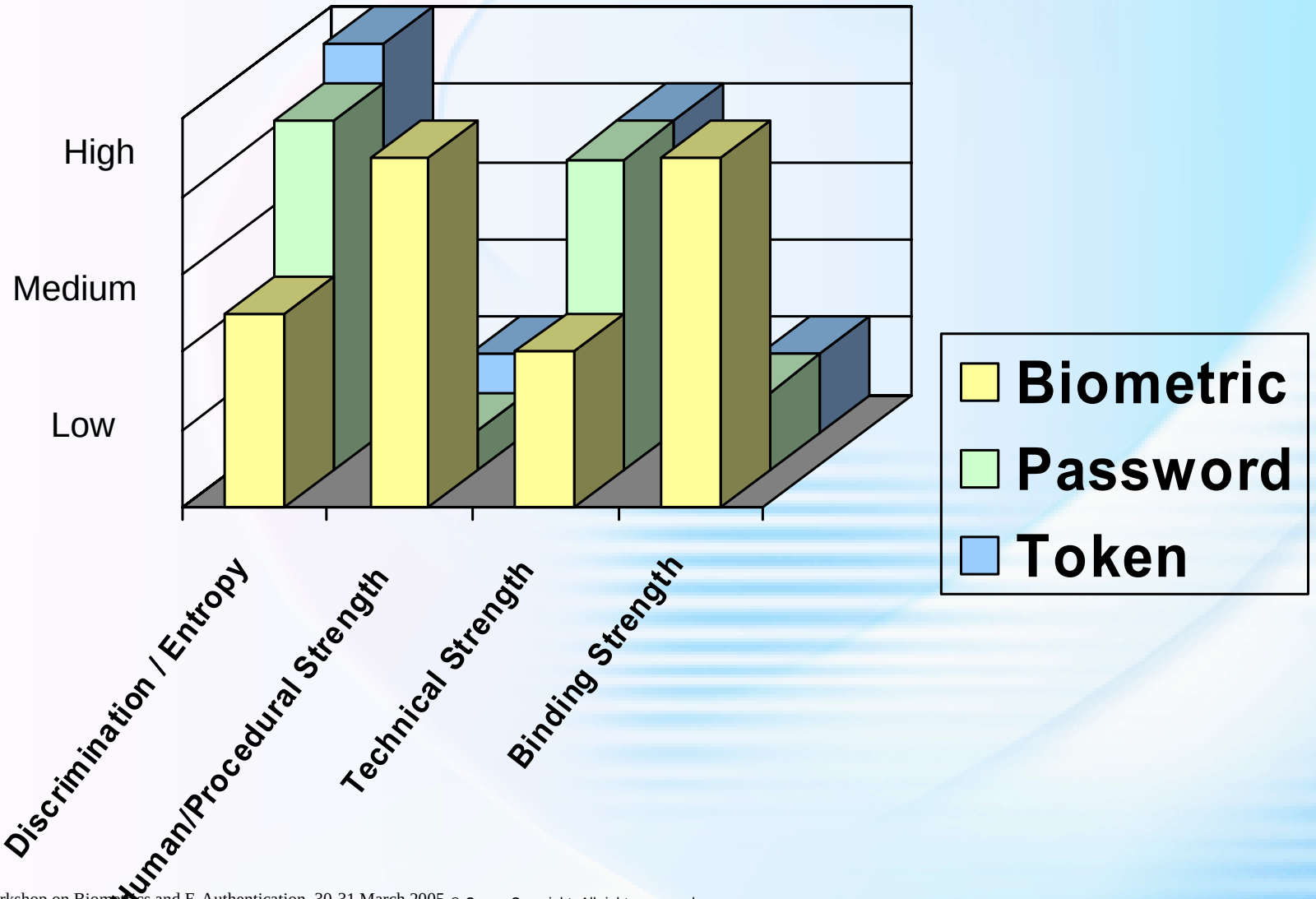
Tokens

- Technically (quite) strong
  - Difficult to copy – physical barriers
  - very difficult to modify – physical and cryptographic barriers
- Procedurally weak
  - Loss
  - Theft
  - But at least you know when it's missing!

Biometrics

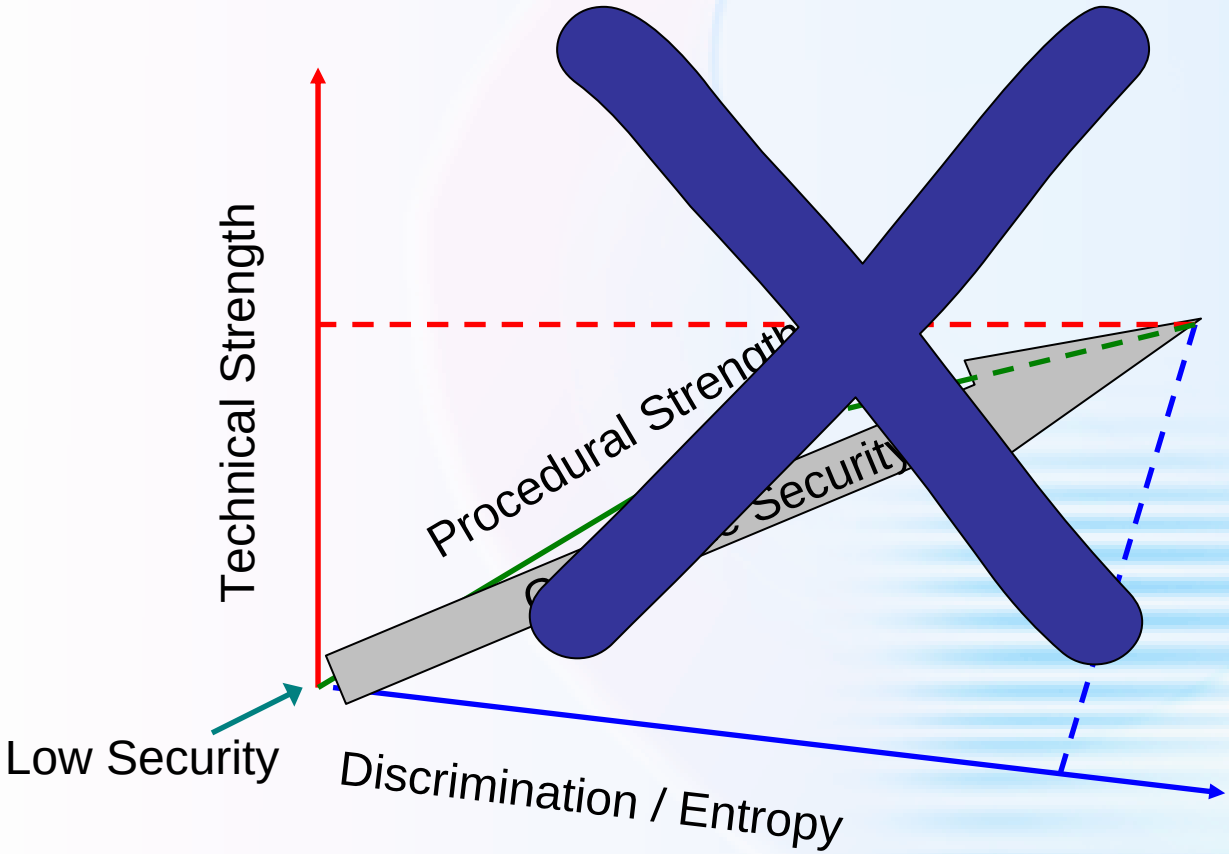
- Technically medium strength (depending on modality)
  - Determined by FAR
    - N.B. Not directly equivalent to password entropy – can't mount exhaustion attack
- Procedurally strong
  - Not reliant on human discipline
- Strong binding of authentication to person
  - N.B. Passwords, Tokens have weak, indirect binding

Comparing Authentication Mechanisms



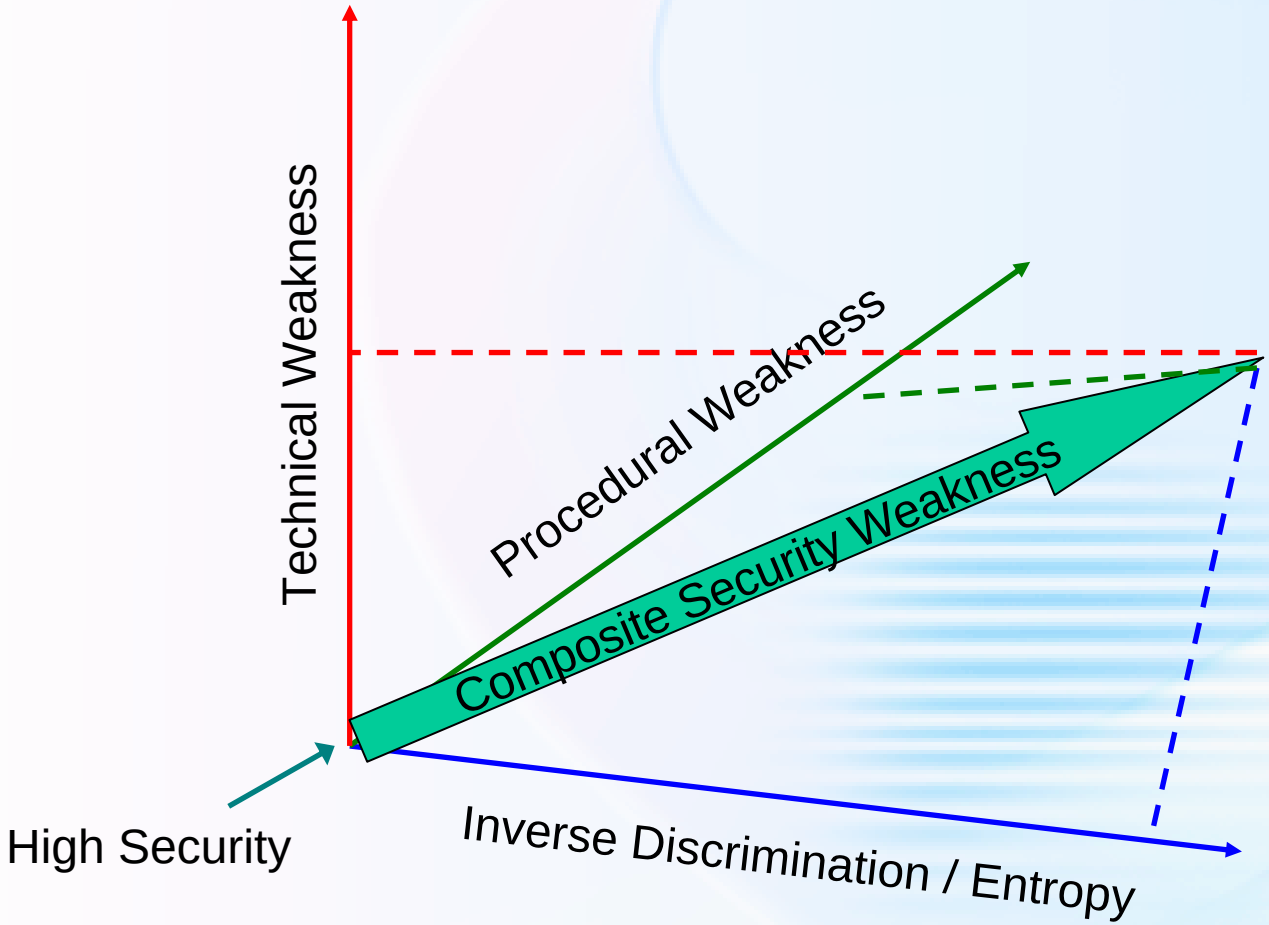
Composite Model for Security

a. Security Strength Vector Approach



Composite Model For Security

b. Security Weakness Vector Approach



Pros and Cons of the “Vector“ Approach

- Accounts for all components that contribute to security
- Provides a more realistic view of the actual security achieved
- Discourages undue emphasis on one element of the security picture

But

- Demands reappraisal of established security paradigms
- Hard to quantify procedural elements
- Difficult to develop / agree comparible scaling of axes.
- Results may conflict with previous cultural “wisdom”

Current UK Government Thinking on Authentication Policy

Brian Holman

CESG ID&A Policy Developer

The Passwords/Biometric Tradeoff

Workshop on Biometrics and E-Authentication Over Open Networks

National Institute of Standards and Technology (NIST)
Gaithersburg, MD

March 30-31, 2005

Presented by Brian Holman CESG UK

Brian.Holman@cesg.gsi.gov.uk

The Passwords/Biometric Tradeoff

This has been developed for internal Government Users (employees), not for citizen-Government, but the approach may be useful for future e-government authentication

Trading off Passwords and Biometrics

Passwords need to be long to make them secure against offline exhaustion attacks

Users don't like long Passwords

So maybe add a Biometric?

Trading off Passwords and Biometrics

?

How should we approach the issue of combining Passwords and Biometrics

Trading off Passwords and Biometrics

We invented a tradeoff rule that simply “feels about right” – calibrated against hypothetical examples

Trading off Passwords and Biometrics

To find a password length we have a UK-specific method for estimating the "Level of Risk" – on a arbitrary scale, then we apply a formula to come up with a Password length

Level of Risk = 1 => typically 6 characters

Level of Risk = 4 => typically 12 characters

But the Level of Risk often goes up to ~6

Trading off Passwords and Biometrics

Adding a biometric system reduces the Level of Risk, and hence indirectly the password length

Trading off Passwords and Biometrics

So we've reduced the problem to characterising a Biometric system into a one dimensional measure:

by how much does the biometric component reduce the level of risk to the password component?

Trading off Passwords and Biometrics

We're weren't sure that it's even sensible to try to reduce characterising a biometric to one dimension - but we did it anyway

The test is "Does it give intuitively sensible answers?"

Trading off Passwords and Biometrics

The characteristic used is a combination of the FAR, a formal Common Criteria assurance measure and a Common Criteria Vulnerability Assessment level – the latter two to ensure there is no obvious weakness such as an easy bypass

Reduction in Risk Level	FAR	EAL	Vulnerability Assessment Level
5	1 in 10^5	5	AVA_VLA.3
4	1 in 10^4	4	AVA_VLA.2
3	1 in 10^3	3	AVA_VLA.2
2	1 in 10^2	2	AVA_VLA.1
1	1 in 10^2	1	None

Trading off Passwords and Biometrics

What it comes out as is that a good Biometric, i.e., a FAR better than 1 in 10^5 , assured to EAL5, will reduce a Password typically by 6 characters; a poor biometric, i.e. FAR ~100, assured to EAL1, will reduce a password by typically 1 character

But we never use less than a 4-digit PIN

Trading off Passwords and Biometrics

We don’t consider the False Rejection Rate

That’s up to each department or agency to decide what is or is not acceptable

Trading off Passwords and Biometrics

As this is new policy – only been out a few weeks – we have no experience of it working in practice, but it seems to make sense

A not-very-good physical analogy

We've replaced one very high but rickety wall with a lower less rickety wall and a moat

?